On page 14, line 11, please change "multiple use" to --multiple-use--.

On page 15, line 13, please change "are offered" to --is offered--.

On page 15, line 18, please change "or a tailor" to --(or a tailor)--.

On page 15, line 18, please change "or style and measurements" to --(or style and measurements)--.

On page 18, line 21, please change "per object" to --per-object--.

On page 18, line 22, please change "paying to the user 103" to --paying--.

IN THE CLAIMS

Please amend claims 1, 5, 14, 19, 22-23, and 25-30 as follows.

---

1. (Twice Amended) A method for automatically disbursing a [user's] first party's personal information to a [requester] receiving party authorized by the [user] first party by transmitting said [user's] first party's personal information from a server computer operated by a service provider, said server computer coupled to a database, the method comprising the steps of:

establishing an account for the [user] first party with the server computer;

assigning an identifier to the [user] first party;

entering the [user's] first party's personal information, said [user's] first party's personal information comprising at least one of a plurality of information objects;

assigning at least one of a plurality of security levels to each information object, thereby enabling access to individually selected portions of the user's personal information by individual receiving parties;

storing in the database the [user] first party identifier, the information object and the security level assigned to the information object;

receiving a request [from a requester], said request [message] comprising at least the [user] first party identifier;

in response to the request, selecting a first portion of the first party's personal information objects that could be transmitted to a receiving party;

retrieving from the database the [information object pertaining to the user identifier] selected first portion of personal information objects; and

securely transmitting the retrieved first portion of personal information objects to the [requester] receiving party.

5. (Amended) The method of claim 1, further comprising the step of recording every access of the [user's] first party's personal information to create an audit trail.

14. (Amended) The method of claim 1, further comprising the steps of:

altering the [user's] first party's personal information; and

storing said altered personal information in the database.

19. (Amended) The method of claim 1, wherein the [user's] first party's personal information includes the [user's] first party's contact information; health–related information; medical, dental information; credit/employment information; insurance information; property–related information; personal demographic information; family medical history; biometric/genetic information; travel/hotel preferences; internet preferences; sartorial, fashion preferences; magazine, movies, book preferences; leisure preferences; preferences for billing or payment methods, or pleasure–related preferences.

22. (Amended) The method of claim 1, wherein the step of receiving a request message from the requester comprises the step of:

receiving a query for the [user's] first party's personal information in a readily executable form.

23. ~~(Amended)~~ The method of claim 1, wherein the step of receiving a request [message] from the [requester] ~~receiving party~~ comprises the step of:

receiving a query for the [user's] first party's personal information in a Structured Query Language format.

25. (Amended) A method for automatically disbursing a [user's] first party's

personal information to a [requesting] receiving party, the method comprising:

step for inputting the [user's] first party's personal information, said [user's] first party's personal information comprising at least one of a plurality of information objects;

step for associating with each information object at least one of a plurality of security clearance levels, thereby enabling access to individually selected portions of the user's personal information;

step for recording each information object and the associated security clearance [levels] level(s);

step for selecting a first portion of the first party's personal information objects that could be transmitted to a receiving party, said selection being made in accordance with criteria established by the first party or in response to a request from the receiving party;

step for inputting an authorization key to access the [user's] first party's personal information;

step for determining a response message to be sent; and

step for outputting the response message.

26. (Amended) [Computer–executable program code stored on computer–readable medium, said code comprising:] A program storage device readable by a processor, said storage device tangibly embodying a program of instructions executable by the processor, said program of instructions comprising:

[code] program of instructions to store a [user's] first party's personal information, said [user's] first party's personal information comprising at least one of a plurality of information objects;

[code] program of instructions to associate each information object with a first security clearance level;

[code] program of instructions to receive a request message to access the [user's] first party's personal information, said request message comprising an authorization key to access a first portion of the [user's] first party's personal information, said authorization key indicative of a second security clearance level;

[code] program of instructions to compare the first security clearance level and

the second security clearance level to determine an appropriate overall clearance level;

[code] program of instructions to match the request message and the overall clearance level with a second portion of the [user's] first party's personal information; and

[code] program of instructions to securely transmit the second portion of the [user's] first party's personal information.

27. (Amended) The [computer–executable program code] program storage device of claim 26, further comprising:

[code] program of instructions to authenticate the request message.

28. (Amended) The [computer–executable program code] program storage device of claim 26, further comprising:

[code] program of instructions to establish a secure audit trail of each access of the [user's] first party's personal information.

29. (Amended) The [computer–executable program code] program storage device of claim 28, wherein the [code] program of instructions to establish a secure audit trail include[s] [code] program of instructions to record an identifier to identify [the requester] a party that receives the first party's personal information.

30. (Amended) The [computer–executable program code] program storage device of claim 28, wherein the [code] program of instructions to establish the secure audit trail [is] are configured to record an identifier to identify the requester.

Please add the following new claims.

31. (New) A computing system comprising a first computer communicatively connected to a communication network and configured (a) to enable a first party connected to the network to store the first party's personal information in a central

repository, said repository operably coupled to the first computer, said first party's personal information including the first party's contact information, and (b) to transmit, in response to a request message received via the network in a standardized protocol format, at least a first portion of the first party's personal information retrieved from the repository, whereby when the first party attempts to do business with or to utilize an offering made by the second party the need to provide said first portion of personal information by the first party to the second party is obviated.

32. (New) The computing system as in claim 31, wherein the repository is a multi-level repository.

33. (New) The computing system as in claim 31, wherein each of the first party's personal information objects is assigned at least one of a plurality of security clearance levels.

34. (New) A service provider-operated centralized multi-level secure repository coupled to a first computer, said first computer coupled to a data communication network, wherein the repository is configured to store at least the first party's identification information, contact information and credit information, wherein each of the identification information, contact information and credit information is assigned at least one of a plurality of security clearance levels, whereby upon receiving, via the communication network, a request and/or a token from a second party, upon verifying the identity of the first party and the authenticity of the second party, the first party's credit information is automatically provided to a designated party, thereby enabling a user to engage in an online commercial transaction.

35. (New) The repository as in claim 34, wherein the security clearance levels are assigned by the first party.

36. (New) The repository as in claim 34, wherein the security clearance levels are assigned by a party other than the first party.

37. (New) A method of securely disbursing a first party's personal information to a second party, the method comprising the steps of:

creating an online repository for the first party's personal information, said personal information comprising the first party's identification information and the first party's credit information;

receiving a request from a second party, the request comprising at least a portion of the first party's identification information and a token, said token configured to enable a single access of the first party's personal information; and

transmitting at least a portion of the first party's credit information to a designated party.

38. (New) The method of claim 37, wherein said authorization key is configured to expire after a predetermined period of time.

39. (New) A communication system comprising:

first storage medium configured to store a first party's personal information, said personal information including a plurality of information objects;

first processor coupled to the first storage medium; and

first memory coupled to the first processor, said first memory configured to store instructions to direct the first processor to download selected portions of the first party's personal information to a second memory responsive to an authorization key, said token configured to enable a single access of the first party's personal information.

40. (New) A method of providing a selected portion of a first party's personal information to a second party comprising the steps of:

receiving a plurality of information objects from the first party at a secure centrally located first computer operated by a service provider;

assigning at least one of a plurality of security clearance levels to each information object;

storing the information objects and the at least one of a plurality of clearance

levels assigned to each information object in a storage device coupled to the first computer;

configuring a token to access a predetermined first portion of the stored information objects within a predetermined expiration time period and/or for a number of times during before the expiration of the predetermined expiration time period, the token providing access to the predetermined first portion of the first party's stored personal information objects to a second party;

receiving a request via a computer network, said request indicative of a subset of stored first party's personal information objects;

electronically presenting the token to the first computer;

determining a security clearance level of the received request;

retrieving a second portion of the predetermined first portion of stored personal information objects that are at or below the security clearance level of the received request; and

transmitting, in an electronic form, information objects so as to enable a form to be filled with data contained in the information objects.

41. (New) A computing system configured to obviate the need for providing a first party's personal information comprising:

a first computer connected to a communication network and configured (a) to enable a first party connected to the network to store the first party's personal information in a central repository, said repository operably coupled to the first computer, said first party's personal information including the first party's identification information, and (b) to transmit, in response to a request message, at least a first portion of the first party's personal information retrieved from the repository, said first portion being the portion authorized to be transmitted in response to the request message, whereby the first portion of the first party's personal information is automatically provided, thereby obviating the need for the first party to provide the first portion of the first party's personal information.

42. (New) The computing system as in claim 41, wherein the repository is a multi–